UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	10 CR. 0096 (DLC)
v.	:	
SERGEY ALEYNIKOV,	:	
Defendant.	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION FOR COURT APPROVAL, *NUNC PRO TUNC*, TO SUBPOENA DOCUMENTS AND MATERIALS FROM GOLDMAN SACHS & COMPANY

MARINO, TORTORELLA & BOYLE, P.C.
437 Southern Boulevard
Chatham, New Jersey 07928-1488
(973) 824-9300
Attorneys for Defendant Sergey Aleynikov

On the Brief:
Kevin H. Marino
John D. Tortorella
John A. Boyle

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Treatises

PRELIMINARY STATEMENT

On this application, Defendant Sergey Aleynikov ("Aleynikov") respectfully seeks Court approval, *nunc pro tunc*, to subpoena the documents and materials described in Exhibit A from Goldman Sachs & Company ("Goldman") for production directly to Aleynikov because he requires those materials to prepare his defense and, most immediately, his pretrial motions.

On June 10, 2010, Aleynikov served a subpoena *duces tecum* upon Goldman with a return date of June 21, 2010. After counsel for Aleynikov and Goldman conferred and failed to agree upon the proper scope and timing of the subpoena (or the propriety of Aleynikov having served the subpoena without prior court approval), counsel for Goldman expressed his intent to challenge the subpoena. Thereafter, Aleynikov's counsel submitted a letter to the Court in which he outlined the history of the subpoena dispute and requested a conference among counsel for the Government, Goldman, and Aleynikov to resolve it. The following day, the Court denied Aleynikov's letter request for failure to comply with Fed. R. Crim. P. 17(c). On June 18, 2010, however, Goldman served an application for an Order to Show Cause why the June 10th subpoena should not be quashed. After receiving Goldman's application, the Court advised the parties and the Government that it would convene a conference on Thursday, June 24th at 9:30 a.m. On this motion, filed with and respectfully submitted to the Court, Goldman, and the Government in advance of the scheduled conference, Aleynikov sets forth the legal and factual bases for the approval and enforcement of the June 10th subpoena.[1]

[1] Courts differ on whether Rule 17(c) imposes a pre-approval requirement. *Compare* United States v. Van Allen, 28 F.R.D. 329, 334 (S.D.N.Y. 1961) ("permission of the court is not needed to serve a subpoena pursuant to Rule 17(c)") *with* United States v. Jenkins, 895 F. Supp. 1389, 1396 (D. Haw. 1995) ("the court believes that Rule 17(c) requires applications for subpoenas…"). Aleynikov issued the June 10th subpoena to

Aleynikov is a computer programmer formerly employed by Goldman. The FBI arrested him on July 3, 2009, and charged him with theft of trade secrets and transportation of stolen property in interstate commerce — to wit, the computer programs that make up Goldman's high-frequency trading platform (the "Platform"). In an Indictment filed on February 11, 2010, Aleynikov was additionally charged with unauthorized computer access based on the same alleged conduct.

Aleynikov's arrest was not the product of a typical FBI investigation. To the contrary, the arrest came just two days after Goldman first apprised the Government of the alleged theft of the Platform and warned that if Aleynikov was not quickly arrested and detained indefinitely, he or others might use the Platform to manipulate world financial markets. To obtain a warrant for Aleynikov's arrest, the Government per force relied on Goldman's representations as to the nature of the computer files Aleynikov downloaded from its computers while still employed there. Those files of course lie at the very heart of the case against Aleynikov. Nevertheless, when Aleynikov sought to obtain the files and other materials underlying the case against him — all of which were compiled in the first instance by Goldman — the Government advised him that

---

Goldman without seeking prior court approval based on Judge Crotty's endorsement of that procedure earlier in this case. (See Exhibit 2 to the Declaration of Kevin H. Marino (hereinafter "Marino Declaration"), (8/10/09 Tr.) at 4:11-24).) Aleynikov respectfully files this curative motion in response to the Court's finding of non-compliance with Rule 17(c) and in keeping with the observation of the court in United States v. Beckford, 964 F. Supp. 1010, 1023 (E.D. Va. 1997) ("Although Rule 17(c) does not explicitly so state, and while there is no controlling authority on this issue, the Court finds that the judicial intervention required by the text of Rule 17(c) and by [Supreme Court case law] can best be accomplished by requiring use of traditionally accepted means to invoke the judicial discretion contemplated by the rule. The usual method to achieve that end is to file a motion and brief explaining why, and on what terms, the court should issue subpoenas duces tecum requiring pre-trial production. This requirement will ensure that the judicial supervision contemplated by subsection (c) occurs at an early stage.")

he would have to subpoena those materials directly from Goldman.

Based on that governmental response to his request for clearly relevant materials, Aleynikov issued, and now seeks Court approval *nunc pro tunc* for, the subpoena *duces tecum* annexed to this memorandum as Exhibit A. First and foremost, Aleynikov requires Goldman to produce the Platform itself, because only by comparing and contrasting the files Aleynikov downloaded from Goldman with the files that constitute the Platform can Aleynikov prove that he did not steal the Platform or any Goldman trade secret, as alleged. As demonstrated below, each item listed on Exhibit A is relevant to Aleynikov's defense of the charges and factual allegations contained in the Indictment, and none will be unduly burdensome for Goldman to produce.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

A. **Background**[2]

Goldman is a financial services firm engaged in, among other things, "high-frequency trading," which "involves the extremely rapid execution of high volumes of trades in which the decisions to make those trades are determined by sophisticated computer programs that use complex mathematical formulas, known as algorithms, to make trading decisions." (Indictment, ¶ 4.) According to the Indictment, Goldman's high-frequency trading activities during the relevant time period were carried out by "a proprietary system of computer programs [(the 'Platform')], which, among other things, rapidly obtained information regarding the latest market

[2] Aleynikov relied upon certain factual allegations from the Complaint and Indictment to provide background solely for purposes of this Motion. He does not thereby accept those facts as true, and he reserves his right to contest any and all such allegations in future motions and at the time of trial.

movements and trends, processed that information into a form that could be analyzed by Goldman's trading algorithms, and then executed the trading decisions resulting from the algorithms." (Id., ¶ 5.)

From May 2007 through June 5, 2009, Defendant Sergey Aleynikov was employed by Goldman as a Vice President in its Equities Division.[3] (Id., ¶ 9.) Aleynikov was a member of the team of computer programmers that was responsible for "developing and improving certain aspects of the Platform." (Id.) Aleynikov left Goldman on June 5, 2009 to join Teza Technologies LLC ("Teza"), a Chicago-based start-up company that intended to develop a high-frequency trading business. (Id., ¶ 2.)

B. The Allegations And Charges Against Aleynikov.

Federal authorities arrested Aleynikov on July 3, 2009, as he exited a plane from a meeting at Teza in Chicago. (Marino Decl., ¶ 2.) Aleynikov was presented on a criminal complaint in the United States District Court for the Southern District of New York on July 4, 2009. (Id.) The two-count complaint charged Aleynikov with theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(2), and transportation of stolen property in foreign commerce, in violation of 18 U.S.C. § 2314. (Complaint.) Those two charges were based on the Complaint's allegation that Aleynikov copied and stole from Goldman the computer source code that constituted the Platform. (Id., ¶ 13.) As the Complaint readily admits, all of the allegations contained therein were based on representations made and documents provided to the Government by representatives of Goldman. (Id., ¶ 5.)

---

[3] Although June 5, 2009, was Aleynikov's last day in the office at Goldman, he continued to be employed by Goldman through June 30, 2009. (Marino Decl., ¶ 2.)

At Aleynikov's initial appearance and detention hearing on July 4, 2009, the Government made a series of representations to the Honorable Kevin N. Fox, U.S.M.J., in an effort to have Aleynikov detained without bail until the conclusion of his trial. (Marino Decl., Ex. 1, 7/4/09 Tr.) Specifically, in an effort to demonstrate that Aleynikov presented a danger to the community in general and Goldman specifically, the Government described the conduct for which he had been charged as the theft of the entire Platform: "What the defendant is accused of having stolen from this investment bank . . . is their proprietary, high-quantity, high volume trading platform with which they conduct all of their trades in all major markets within the United States and other places." (Id. at 7:7-12.) At several points throughout the hearing, the Government stressed that the Complaint accused Aleynikov of stealing the entire Platform, not just discrete portions of it. (Id. at 16:16-18 ("I should put that there's never been any breaches in anywhere of this magnitude before of the bank where the entire platform has gone out."); id. at 17:8-9 ("the entire platform has been stolen"). The Government argued that, because Aleynikov had stolen the entire Platform, he presented a significant risk to the community if released because he (or someone to whom he might transfer the purportedly stolen material) could readily and without delay use the Platform "to manipulate markets in unfair ways." (Id. at 8:6-7.) In other words, the Government represented to Judge Fox not just that Aleynikov had stolen part of Goldman's trading Platform, but that he had stolen all of it and, as a result, was in a position if released from custody to quickly implement the Platform elsewhere and manipulate and cause damage to the world financial markets. (These representations about the Platform's capacity, and therefore Goldman's, to manipulate world financial markets were delivered without apparent irony.)

The transcript of the July 4th detention hearing reveals that the statements made by the Government to the Court regarding the nature and import of what Aleynikov purportedly did were based entirely upon Goldman's representations. (Id. at 24:20-25:9.) Indeed, the transcript confirms that (a) Goldman first contacted the Government on Wednesday, July 1, 2009, just two days before Aleynikov's arrest (id. at 33:6-9); and (b) the Government did not verify Goldman's claims — that Aleynikov had misappropriated its entire high-frequency trading Platform and thus presented a significant risk to the world financial markets — before arresting him and seeking to have him detained indefinitely without bail.

In a three-count indictment filed with this Court on February 11, 2010 (the "Indictment"), seven months after Aleynikov's hasty arrest, the Government charged him with the following offenses: (1) theft of trade secrets in violation of 18 U.S.C. §§ 1832(a)(2) and (a)(4); (2) transportation of stolen property in interstate and foreign commerce in violation of 18 U.S.C. § 2314; and (3) unauthorized computer access and exceeding authorized computer access in violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i)-(iii). The core allegation underlying the Indictment's charges against Aleynikov was that, on June 5, 2009, he "without authorization copied and transmitted to his home computer Goldman's proprietary computer source code for Goldman's high-frequency trading business, with the intent to use that source code for the economic benefit of himself and his new employer, Teza." (Indictment, ¶ 16; see also ¶ 18 (alleging that Aleynikov stole, converted and took "Goldman's proprietary computer source code for Goldman's high-frequency trading business, . . . uploaded the code to a computer server in Germany, and carried that stolen code to a meeting with his new employer, Teza, in Chicago, Illinois"). The Indictment does not allege (just as the Complaint did not) that in the month

between his alleged taking of the Platform on June 5, 2009 and his arrest on July 3, 2009, Aleynikov transferred, made any effort to transfer or offered to transfer any portion of the material he allegedly copied to Teza or any other entity. Indeed, the Indictment makes no allegation that Aleynikov ever made any effort to use the copied material in any capacity in the month prior to his arrest.

The Indictment alleges that Aleynikov accomplished the theft of the Platform by utilizing a computer script he wrote and stored on his work computer that, when executed, copied certain Goldman files and compressed them into a single file. (Indictment, ¶ 12.) The Indictment alleges that Aleynikov improperly and without authorization transferred source code for Goldman's high-frequency trading system to his home computers on many occasions prior to his last day of work at Goldman. (Id., ¶ 14.) According to the Indictment, after Aleynikov copied and compressed the subject source code on June 5th, he transferred the compressed file from Goldman's network to a server in Germany. (Id.) The server was associated with a website that offered services to computer programmers who wished to store their source code projects there. (Indictment, ¶ 12(b).) Thereafter, Aleynikov accessed the website from his home in New Jersey and downloaded the source code to his home computer; several days later, he copied some of the files to other home computers, including a laptop, and to a portable flash drive. (Id., ¶ 13.)

On July 2, 2009, Aleynikov traveled to Chicago to attend meetings at Teza's offices. (Id., ¶ 15.) Aleynikov allegedly brought to the meeting the laptop computer and flash drive containing source code for Goldman's high-frequency trading system, including some of the source code that he allegedly copied and transferred. (Id.) The Indictment does not allege that, while in Chicago, Aleynikov transferred or offered to transfer any of the source code to Teza.

Again, the Indictment is devoid of any allegation that, in the month between his alleged taking of the Platform on June 5, 2009, and his arrest on July 3, 2009, Aleynikov transferred, made any effort to transfer or offered to transfer to Teza or any other entity any portion of the source code he allegedly copied.

In support of the contention that the files allegedly misappropriated by Aleynikov constituted trade secrets, the Indictment alleged that Goldman had taken various measures to protect the high-frequency trading system's source code. (Indictment, ¶ 8.) Specifically, Goldman allegedly (1) maintained a firewall designed to prevent outsiders from accessing information on its computer network; (2) limited access to the Platform's source code to only those employees who had reason to access the code; (3) blocked certain transfers of information from its network; (4) monitored some transfers of information by employees from the network; and (5) required all Goldman employees to agree to a confidentiality agreement. (Id.)

C. Aleynikov's Efforts To Obtain the Requested Information From The Government And Goldman.

In May 2010, in anticipation of engaging expert witnesses and drafting pretrial motions on Aleynikov's behalf, his newly-retained counsel requested that the Government provide Aleynikov with various materials counsel believed the Government had or should have received from Goldman prior to charging him. (Marino Decl., ¶ 3.) The requested materials included much technical data regarding the Platform as well as ancillary materials Goldman gathered and conveyed to the Government in making its referral. (Id.) After considering Aleynikov's counsel's request, the Government advised that it would not provide the requested materials and informed counsel that if he wished to obtain the materials, he would have to subpoena them from

Goldman itself. (Id., ¶ 4.)

Upon receiving that advice from the Government, Aleynikov's counsel promptly prepared a subpoena and, on June 8, 2010, contacted Matthew Friedrich, Esq., a partner at Boies, Schiller & Flexner, to ask that he accept service of that subpoena on Goldman's behalf. (Id., ¶ 5.) Counsel was aware of Mr. Friedrich's representation of Goldman because he moved unsuccessfully before Judge Crotty to quash an earlier subpoena served upon Goldman by Mr. Aleynikov's prior counsel, Assistant Federal Public Defender Sabrina Schroff for, inter alia, failure to comply with Rule 17(c). (Id., ¶ 5 & Ex. 2.) Mr. Friedrich agreed to bring Aleynikov's service request to Goldman and the following day, June 9, 2010, advised counsel that Aleynikov would be required to serve Goldman directly. (Id., ¶ 6.)

On June 10, 2010, Aleynikov's counsel served upon Goldman a subpoena *decus tecum* with a return date of June 21, 2010.[4] (Id., ¶ 7 & Ex. 3.) Thereafter, Mr. Friedrich called to advise Aleynikov's counsel that the subpoena had made its way to him; that he planned to move to quash it; and that he would like Aleynikov to agree to a non-emergent briefing schedule on that motion. (Id., ¶ 8.) Aleynikov's counsel advised Mr. Friedrich of the impending July 16th deadline for the filing of pretrial motions and indicated that, given that deadline, he could not agree to his request. (Id.) Aleynikov's counsel also offered to meet with Mr. Friedrich to entertain his suggestions for narrowing the subpoena; gave him a summary of Aleynikov's reasons for needing each of the subpoenaed documents; and advised him that Aleynikov had no objection to the entry of a protective order to safeguard any interest Goldman might have in the

[4] The items subpoenaed on June 10th were substantially the same as the items set forth on Exhibit A, with the exception of two typographical errors that have been corrected.

confidentiality of any of the subpoenaed documents. (Id., ¶ 9.)

When Mr. Friedrich responded that he intended to bring this matter before the Court, Aleynikov's counsel advised that he would write a letter to the Court outlining the dispute from Aleynikov's perspective. (Id., ¶ 10.) On June 16, 2010, Aleynikov's counsel submitted a letter to the Court in which he outlined the history of the subpoena dispute and requested a conference among counsel for the Government, Goldman and Aleynikov to resolve it. (Id., ¶ 10 & Ex. 4.) On June 17, 2010, the Court docketed an endorsed copy of Aleynikov's June 16th letter indicating that it had been denied for failure to comply with Rule 17(c). (Id., ¶ 11.) On June 18, 2010, Goldman, through Mr. Friedman, served Aleynikov's counsel with an application for an Order to Show Cause why the June 10th subpoena should not be quashed. (Id., ¶ 12.) Goldman's application argued that the subpoena was defective because, among other reasons, Aleynikov failed to obtain leave of court before serving it. (Id.) This motion follows.

LEGAL ARGUMENT

II. LEGAL STANDARD.

The Sixth Amendment to the United States Constitution affords an accused the right to compulsory process. U.S. Const. Amend. VI. That right includes, at a minimum, "the right to the government's assistance in compelling the attendance of favorable witnesses at trial and the right to put before a jury evidence that might influence the determination of guilt." Pennsylvania v. Ritchie, 480 U.S. 39, 56 (1987). It is well settled that the Sixth Amendment guarantee of compulsory process is fundamental to the right to a fair trial. Washington v. Texas, 388 U.S. 14, 18-19 (1967). As the Supreme Court has explained, compulsory process in criminal cases is essential for the proper functioning of our criminal justice system:

> We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense.

United States v. Nixon, 418 U.S. 683, 709 (1974).

Rule 17(c) implements the Sixth Amendment right to compulsory process by providing for the issuance of subpoenas in criminal cases to enable an accused to secure evidence in his favor. In re Martin Marietta Corp., 856 F.2d 619, 621 (4th Cir. 1988); United States v. Garmany, 762 F.2d 929, 933-34 (11th Cir. 1985); Charles Alan Wright and Peter J. Henning, 2 Fed. Prac. & Proc. Crim. § 271. In particular, Rule 17(c)(1) governs the issuance of subpoenas *duces tecum* in federal criminal proceedings and expressly provides for subpoenas requiring the production of documents and other materials on a return date in advance of actual trial. Nixon, 418 U.S. at 697-98. The rule provides as follows:

> A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Fed. R. Crim. P. 17(c)(1).

Although the Supreme Court has stated that a Rule 17(c) subpoena *duces tecum* is "not

intended to provide an additional means of discovery," it also recognized that "[i]ts chief innovation was to expedite the trial by providing a time and place *before* trial for the inspection of the subpoenaed materials." Nixon, 418 U.S. at 698-99 (quoting Bowman Dairy Co. v. United States, 341 U.S. 214, 220 (1951)) (emphasis in original); see also Fed. R. Crim P. 17(c)(2).

In considering the appropriate standard for a request by ***the prosecution*** for a Rule 17(c) subpoena, the Supreme Court in Nixon recognized that courts have required the following showing:

> (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general "fishing expedition."

Nixon, 418 U.S. at 699-700. Against this backdrop, the Supreme Court distilled the test to three parts: (1) relevancy; (2) admissibility; and (3) specificity. Id. at 700.

More recently, in United States v. Nachamie, 91 F. Supp. 2d 552 (S.D.N.Y. 2000), Judge Scheindlin considered whether the Nixon standard ought to apply to a ***defense*** subpoena of documents from third parties. The court framed the issue as follows:

> That high standard, of course, made sense in the context of a Government subpoena, especially one seeking evidence from the President. It must be recalled that the Government's use of a subpoena occurs *after* the completion of a grand jury investigation. Indeed, the Supreme Court has held that "the Nixon standard does not apply in the context of grand jury proceedings . . . ." United States v. R. Enterprises, 498 U.S. 292, 299-300, 112 L.Ed.2d 795, 111 S.Ct. 722 (1991). A real question remains as to whether it makes sense to require a defendant's use of Rule 17(c) to obtain material from a non-party to meet this same standard. Unlike the Government, the defendant has not had an earlier opportunity to

> obtain material by means of a grand jury subpoena. Because the Rule states only that a court may quash a subpoena "if compliance would be unreasonable or oppressive," the judicial gloss that the material sought must be evidentiary — defined as relevant, admissible and specific — may be inappropriate in the context of a defense subpoena of documents from third parties.

Nachamie, 91 F. Supp.2d at 562-63. Judge Scheindlin, therefore, formulated a two-part test for defense subpoenas: "whether the subpoena was (1) reasonable, construed using the general discovery notion of 'material to the defense,' and (2) not unduly oppressive for the producing party to respond." Id. This test has been employed in subsequent decisions, see United States v. Von Tucker, 249 F.R.D. 58, 66 (S.D.N.Y. 2008); United States v. Soliman, No. 06CR236A, 2009 U.S. Dist. LEXIS 45194, at **9-13 (W.D.N.Y. May 20, 2009).[5]

A document is considered material if "it could be used to counter the government's case or to bolster a defense." United States v. Stevens, 985 F.2d 1175, 1180 (2d Cir. 1993). Stated differently, "[e]vidence is material if its pretrial disclosure will enable a defendant to alter

---

[5] At least one noted scholar on federal criminal practice also shares the view that application of the Nixon test to defense subpoenas is inappropriate:

> Nixon is a reasonable standard to apply to *prosecutors* who seek additional evidence to bolster their case, having already gathered sufficient information to decide to seek an indictment and commence the process leading to a criminal trial. . . . Applying the identical standard to defendants is wrong because they have none of the investigatory advantages of the government, nor the means to compel the production of items about which they may not have a significant amount of information. . . . Nixon imposed a high standard, but not because the language of Rule 17 (c) either demands or implies that every party using a subpoena for pretrial production must establish relevancy, admissibility and specificity to compel the production of documents.

Peter J. Henning, Federal Discovery Part 2: Defense Discovery in White-Collar Criminal Prosecutions: Federal Rule of Criminal Procedure in Subpoenas, 23 Champion 26, 66 (December 1999) (emphasis in original).

significantly the quantum of proof in his favor."[6] United States v. Giffen, 379 F. Supp. 2d 337, 342 (S.D.N.Y. 2004). A defendant establishes that a subpoena request is material to the defense by, inter alia, demonstrating a connection between his requests and his defense, including any defenses argued in a motion to dismiss an indictment and general defenses to be propounded at trial (such as any defense that might lead to a showing of reasonable doubt as to guilt). Soliman, 2009 U.S. Dist. LEXIS 45194, at **11-12.

A defense subpoena will not be deemed oppressive merely because the documents sought are voluminous, substantial expense may be incurred in their production, or there may be a disruption caused by their production. See In re Subpoena Duces Tecum (Bailey), 228 F.3d 341, 350-51 (4th Cir. 2000). Further, where a defendant's requests are targeted to ensure production of material evidence, a subpoena will not be considered oppressive. Soliman, 2009 U.S. Dist. LEXIS 45194, at **12-13 (granting a defendant's application for subpoenas where his requests, although potentially voluminous, were targeted to ensure production of material evidence).

As demonstrated below, applying the Nachamie standard, each of the specific items requested in Aleynikov's proposed subpoena are material to his defense and not unduly burdensome. Accordingly, he should be granted leave *nunc pro tunc* to serve the subpoena upon

---

[6] Similarly, relevance means that the items sought "would tend to prove a material issue of the prosecution or defense." United States v. Grant, No. 04 Cr. 207, 2004 U.S. Dist. LEXIS 28176, at *3 (S.D.N.Y. Nov. 18, 2004). Documents will also be considered relevant if they relate to charges in an indictment. See United States v. Gross, 24 F.R.D. 138, 140 (S.D.N.Y. 1959).

Goldman.[7]

III. BECAUSE THE DOCUMENTS AND MATERIALS REQUESTED IN THE PROPOSED SUBPOENA ARE MATERIAL TO THE DEFENSE AND ARE NOT UNDULY OPPRESSIVE, ALEYNIKOV SHOULD BE GRANTED LEAVE TO SERVE THE SUBPOENA.

For the reasons set forth below, each of the items identified on the attached Exhibit A satisfies the Nachamie standard:

1. All computer files, programs, source code and other components comprising the high-frequency trading system (the "Platform") of Goldman Sachs & Co. ("Goldman").

In order to counter the allegation that Aleynikov stole Goldman's high-frequency trading platform, the defense must have access to the Platform itself — the alleged trade secret he is charged with stealing. Because Aleynikov is charged with theft of trade secrets, he is "entitled to all materials comprising the trade secrets identified in the indictment in preparing [his] defense." United States v. Lee, No. 5:06 CR 0424 JW, 2009 U.S. Dist. LEXIS 24972, at *7 (N.D. Cal. Mar. 18, 2009). Indeed, there could hardly be data more material and critical to the defense than the very "trade secret" at the heart of the prosecution. Only by comparing the Platform to the files actually downloaded by Aleynikov will defense experts be able (1) to explain to a fact-finder that Aleynikov did not actually take the Platform; and (2) to distinguish the non-proprietary materials Aleynikov downloaded from the arguably proprietary materials that may compose other portions of the Platform. In addition, the defense needs access to the Platform to analyze and explain how any code Aleynikov downloaded functioned within Goldman's system. Further, the production of the entire Platform is critically material to issues of intent because an

[7] Even if the Court were to apply the Nixon standard in this context, the subpoena readily satisfies that standard as to each category of requested information.

analysis of the entire Platform will enable the defense expert to testify that any discrete portions of the Platform Aleynikov copied were of little value as compared to other components that he could have, but did not, copy.

Although the code that composes the Platform may be voluminous, this request is not unduly burdensome because it specifically requires production of the very trade secret that Goldman claimed had been stolen. Soliman, 2009 U.S. Dist. LEXIS 45194, at **12-13. In its application for an order to show cause, Goldman takes issue with this request and others simply because of their use of the word "all." (OTSC Br. at 10.) But a subpoena need not "designate each particular paper [or thing] desired" so long as the "kinds of documents are designated with reasonable particularity." Charles Alan Wright and Peter J. Henning, 2 Fed. Prac. & Proc. § 275 (4th ed.). Here, although Aleynikov requests *all* documents of a particular type, he identifies with great specificity the materials requested — namely, all those files that constitute the Platform he is charged with stealing. As the owner of the Platform, Goldman needs nothing further to know precisely what material is responsive to Aleynikov's request.

Finally, given the complexity of the Platform, the defense requires production of it now to ensure that Aleynikov's experts have sufficient time to perform the required analysis prior to trial. This request is also directly relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

2. Documents sufficient to evidence any and all measures taken by Goldman to maintain the secrecy, confidentiality and/or proprietary nature of the programs, files, source code and other components comprising the Platform.

In order to demonstrate that the code Aleynikov downloaded constituted a trade secret — as the Government must to establish that he violated the Economic Espionage Act — it must

prove beyond a reasonable doubt that Goldman took reasonable measures to keep the information secret. United States v. Shiah, No. SA CR 06-92, 2008 U.S. Dist. LEXIS 11973 (C.D. Cal. Feb. 19, 2008). Indeed, the Government acknowledges that it bears that burden, as the Indictment contains a full page of allegations detailing the measures Goldman purportedly took to protect the source code for its high-frequency trading system. (Indictment, ¶ 8(a)-(d).) Those alleged measures included installing firewalls to keep outsiders from gaining access to Goldman's system; placing limitations on the access granted to Goldman insiders; and constructing mechanisms to block and monitor the transfer of data outside of Goldman. (Id.) To put Aleynikov's expert in a position to challenge the reasonableness of Goldman's security measures during his testimony, the defense must have documents from Goldman sufficient to evidence the measures the company actually took to keep the Platform secret.

This request is highly specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's motion that there is not sufficient evidence to support the Indictment.

3. All documents relating to any employee training provided by Goldman regarding the identification and protection of confidential and/or proprietary information and material.

Documents relating to the training of Goldman employees regarding the identification and protection of confidential information also constitute material, relevant evidence necessary for the defense to demonstrate that Goldman did not take reasonable security measures and, therefore, that the Government cannot establish an EEA violation. In fact, the district court in Shiah specifically discussed the relevance of a company's confidentiality training — and commented on the inadequacy of the training in the case before it — when analyzing whether the

Government had proven the reasonable-measures element of the trade secret charge in the case before it. 2008 U.S. Dist. LEXIS 11973 at *63-64. In addition, the materials requested in Item 3 will enable the defense to demonstrate that Goldman did not adequately identify the code downloaded by Aleynikov as confidential or containing trade secrets, which is relevant to both the reasonable-measure element and whether Aleynikov had the intent to steal trade secrets.

These specifically-identified materials are not obtainable from any source other than Goldman. Goldman has stated that it is prepared to produce materials responsive to this request upon entry of a satisfactory protective order. (Mem. in Support of OSC at 5.) This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

4. All confidentiality and/or non-disclosure agreements that Sergey Aleynikov ("Aleynikov") executed or to which he was otherwise bound during his employment by Goldman.

Like Items 2 and 3, confidentiality and non-disclosure agreements by which Aleynikov was bound during his employment are relevant to enable the defense to demonstrate the inadequacy of Goldman's efforts to protect its alleged trade secrets. In that regard, the existence and adequacy of a confidentiality agreement was deemed by the district court in Shiah to be of critical importance to the reasonable-measures issue. 2008 U.S. Dist. LEXIS 11973 at *63-64. Here, the Government alleges in the Indictment that at least one confidentiality agreement to which Aleynikov was purportedly bound during his employment constitutes one of the reasonable measures Goldman took to protect the Platform's source code; in fact, the Government actually quotes several phrases alleged to come from that agreement. (Indictment, ¶ 8(d).) As a result, it is critical to Aleynikov's defense that he and his experts (1) have the

opportunity to analyze that agreement; and (2) know whether any other such agreements exist.

Moreover, this Item calls for the production of a discrete group of documents that would not be unduly burdensome to produce. Indeed, Goldman stated that it was prepared to produce materials responsive to this request upon entry of a satisfactory protective order. (Mem. in Support of OSC at 5.) This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

5. All written confidentiality and/or non-disclosure policies of Goldman that were effective during Aleynikov's employment by Goldman, including but not limited to all policies mandating or evidencing any mandatory confidentiality legends required to accompany source code containing trade secrets.

Aleynikov requires access to the confidentiality and non-disclosure policies described in this request so he can demonstrate the inadequacy of Goldman's efforts (i) to protect its alleged trade secrets; and/or (2) to advise its employees of the substance and contours of those policies. Because this Item requests written policies for requiring confidentiality legends to be included on proprietary code, the defense will use the responsive material to show at trial that Goldman's failure to comply with those policies and procedures demonstrates that it did not consider the code Aleynikov transferred to contain proprietary information. Alternatively, Aleynikov will be able to demonstrate that his conduct did not, in fact, violate Goldman's confidentiality and non-disclosure policies or that he reasonably believed his conduct conformed to those policies and procedures. In any event, Aleynikov should be granted access to the documents sought in Request No. 5 because they form an integral part of the charges against him. In that regard, the Indictment itself alleges in numerous places that Aleynikov's actions violated Goldman policies and procedures. (Indictment, ¶¶ 8(d), 14.) The substance of those policies is thus extremely

important to the defense.

In United States v. Caruso, 948 F. Supp. 382 (D.N.J. 1996), a former partner of Coopers & Lybrand, LLP ("C&L") sought, via a Rule 17(c) subpoena, documents concerning certain C&L policies and practices; the defendant argued that he needed the documents to establish a state-of-mind defense because his actions were appropriate in light of C&L policy and practice. Id. at 396. The court concluded that the defendant was entitled to the documents because they were "clearly evidentiary, relevant and admissible." Id. at 397. The court found that the documents were relevant to establishing the defendant's state of mind at the time of the offense and, as such, would be admissible at trial. Further, the court found that the defendant's ability to prepare for trial would be compromised without the subject documents, and that the trial would be unreasonably delayed based on defense counsel's representations that the defendant would not be able to open to the jury without first having had an opportunity to review the documents. Id.

Finally, the court found that the defendant's requests were reasonably specific and did not appear to be a bad faith 'fishing expedition.'" Id. In so finding, the court noted that the subpoena was targeted at uncovering specific documents or types of documents that were relevant to establishing a potential defense. Id. at 399. The court stated that the subpoena was as specific as could reasonably be expected under the circumstances (that is, where the defendant did not actually possess the documents, but had knowledge as the former managing partner about what the documents would purportedly contain). Id. Likewise here, Goldman's confidentiality and non-disclosure policies are material to the defense, as evidenced most clearly by the Indictment's numerous explicit references to them.

6. All written policies of Goldman regarding the copying and/or use of computer source code, files and programs for working at home or otherwise outside of Goldman's premises that were effective during Aleynikov's employment by Goldman.

Like Items 2 through 5, the information sought by this request will enable the defense to demonstrate that Goldman's efforts to protect its alleged trade secrets were not adequate. The defense will show at trial that the files Aleynikov actually downloaded on his last day at Goldman were identical to files he had downloaded periodically throughout his tenure at Goldman. To the extent Goldman had any policies against copying and/or using computer source code, files and programs for working at home, the defense will demonstrate that Goldman did not enforce them during Aleynikov's employment. Alternatively, Aleynikov will demonstrate that either that his conduct was entirely consistent with those policies or that he was reasonable in believing that it was. Moreover, as with the policies sought in Item 5, the Indictment specifically alleges that Aleynikov breached the policies sought in Item 6; he thus has a right to review those policies. This is a request for a specific group of policies that will not present any burden to produce. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

7. All written policies or procedures of Goldman relating to determining whether departing employees are in possession of any proprietary, confidential or trade secret information or material that were effective during Aleynikov's employment by Goldman.

Like Items 2 through 6, the information sought by this request will enable the defense to demonstrate that Goldman did not adequately protect any non-public information in its possession. The defense will show that if Goldman had policies relating to determining whether departing employees were in possession of any proprietary, confidential or trade secret

information or material, it did not abide those policies. If no such policies exist, it will constitute further evidence that Goldman did not adequately protect any non-public information in its possession. For example, in Shiah, the court noted as a deficiency in the company's reasonable measures that it failed to inspect the defendant's computer upon his departure from the company. Shiah, 2008 U.S. Dist. LEXIS 11973, at **65-66. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

8. All communications between Goldman and Teza Technologies LLC relating to Aleynikov and/or the Platform.

9. All communications between Goldman and the Federal Bureau of Investigations or the United States Attorney's Office for the Southern District of New York relating to Aleynikov and/or the Platform.

10. All documents relating to any investigation conducted by Goldman of Aleynikov and his alleged theft of the Platform.

In Items 8, 9 and 10, Aleynikov seeks documents relating to Goldman's internal investigation and its communications with the FBI, the U.S. Attorney's Office, and Teza Technologies LLC concerning Aleynikov and his alleged theft of the Platform. The documents sought are highly relevant to this prosecution. First, the requested documents are relevant to the issue of whether the data allegedly copied by Aleynikov constituted a trade secret within the meaning of the EEA. For this information to qualify as a trade secret, the Government must prove, inter alia, that Goldman had "taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3); Shiah, 2008 U.S. Dist. LEXIS 11973, at *56. In the Indictment, the Government asserts that such measures included "monitoring some transfers of information by employees outside of Goldman's computer network" (Indictment, ¶ 8(c)); indeed, it was during just such routine monitoring that Goldman allegedly discovered the transfers by Aleynikov.

(Compl., ¶ 7; 7/4/2009 Detention Hearing Tr. at 33:2-8; 38:16-19.)

Second, the requested materials relate to communications concerning an internal investigation conducted by Goldman into the very activities that form the basis of the Indictment. See United States v. Reyes, 239 F.R.D. 591, 599 (N.D. Cal. 2006) (finding that an audit committee's internal investigation was relevant to the defendant's prosecution). Here, as the Complaint makes clear, the Government's entire "investigation," and consequently this entire prosecution, was based on representations made and documents provided by Goldman to the Government.

Other actions or inactions Goldman took upon Aleynikov's departure from the company are likewise relevant to the reasonableness inquiry. As noted above, in Shiah, one of the deficiencies in the company's protective measures was its failure to inspect the defendant's computer upon his departure. Shiah, 2008 U.S. Dist. LEXIS 11973, at **65-66. Accordingly, the documents relating to Goldman's internal investigation, including its monitoring of transfers, are relevant to the EEA charge.

Moreover, the requests satisfy the specificity requirement because Aleynikov "demands access to a discrete set of existing written materials, within the possession of the subpoenaed parties, that pertain to events and conversations that actually occurred and relate to specific subject matter." Reyes, 239 F.R.D. at 599. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

11. The content of the https logs from the proxy server containing records from 3/1/2009 to 6/5/2009 showing originating and destination IPs (and host names) and the size of transferred data.

12. The IP addresses of all tws-spice-c1 through tws-spice-c12 machines and qtdev1 through qtdev6 machines as of 3/1/2009, 4/1/2009, 5/1/2009 and 6/5/2009.

The Indictment alleges that Aleynikov transferred more data on his final day of work than he had ever transferred previously. The logs and IP addresses requested in Item 11 and 12 will identify the data actually transferred on Aleynikov's last day and from where the data originated. These materials will enable a defense expert to determine whether Aleynikov transferred the same files with regularity and whether each transfer was of comparable size and composition. Items 11 and 12 are also necessary to establish that Aleynikov did not exceed his authorized access, as alleged in Count 3 of the Indictment.

These requests are very specific and the Items requested are not obtainable from any source other than Goldman. These requests are also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

13. The full content of all files and subdirectories of the /bld/dev directory as of 6/5/2009.

14. A full recursive list of all files found in the directory and all subdirectories of /bld/pre (showing file path, file name, file size, access permission mask, group name, and user name) as of 6/5/2009.

15. A full recursive list of all files found in the directory and all subdirectories of /bld/ver (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

16. A full recursive list of all files found in the directory and all subdirectories of /bld/prod (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

Items 13 through 16 are necessary to demonstrate that Aleynikov did not intend to

convert Goldman's alleged trade secrets to his or anyone else's economic benefit — an element the Government must prove beyond a reasonable doubt to establish an EEA violation. 18 U.S.C. § 1832(a)(2). A comparison of the requested Items with the files Aleynikov actually downloaded will demonstrate that, to the extent he downloaded code, he only downloaded versions of code that were under development. The defense will show at trial that Goldman Sachs puts code through three stages of development before putting it into service. Code in the /dev directory is under development. This is akin to a rough draft. Code in the /pre directory is stable code that is in pre-production. Code in the /ver directory is the next version anticipated to be released into production. Code in the /prod directory is the current, working version of the software that is in service. Aleynikov's script copied only unstable code from the /dev directory. The defense will show that Aleynikov did not copy files from the /ver, /prod or /pre directories, even though changing a few characters in his script would have enabled Aleynikov to copy the stable source code used for producing production-quality software used by Goldman for its Platform. These Items will therefore enable the defense to show that if Aleynikov had intended to get a monetary benefit from transferring the code, he could have and would have downloaded production versions of the code. This request is very specific and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

17. The full content of all files and subdirectories of the /sw/external/erlang-common directory as of 6/5/2009.

18. The full content of all files and subdirectories of the /sw/external/erlang directory as of 6/5/2009.

The Indictment alleges that Aleynikov "executed the transfer of hundreds of thousands of

lines of source code for Goldman's high-frequency trading system from Goldman's computer network, including files relating to both the Platform and the trading algorithms." (Indictment ¶ 12.) The directories requested in Items 17 and 18 contain third-party and open source code, not proprietary information. The defense requests the contents of these directories so that it can demonstrate that these files, which were part of Aleynikov's user account and download, do not contain proprietary information. This request is very specific and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

19. A full recursive list of all dependencies of the twscore and tsecdb packages as of 6/5/2009.

The defense will demonstrate at trial that the Platform consisted of several packages, two of which are "twscore" and "tsecdb". To build and use a package, one needs all files on which the package depends. The defense requires the list requested in Item 19 to show that what Aleynikov downloaded was not sufficient to build a package. For example, Aleynikov may have downloaded element A, but one would need elements B, C, and D (which he did not download) to construct the package. The information sought through this request, therefore, is relevant to demonstrate that Aleynikov did not intend to convert the alleged trade secret to his or anyone else's economic benefit — an element the Government must prove beyond a reasonable doubt to establish an EEA violation. 18 U.S.C. § 1832(a)(2). This request is very specific and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

20. A full recursive list of all files found in the directory and all subdirectories of /sw/external (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

The defense will establish that this directory was a repository for third-party and open source projects (i.e., non-proprietary information). This list will enable Aleynikov to establish that he maintained some of the open source projects present in his download and did not exceed his authorized access. This request is very specific and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

21. All MS Communicator chat records of the aleyns account between 5/20/2009 and 6/5/2009.

The defense will demonstrate at trial that Aleynikov regularly transferred files offsite and to a local directory on hosts at Goldman's development network so that he would be able to continue working productively in case of a network outage at Goldman to servers hosting repositories with platform source code. The records requested in Item 21 will demonstrate that shortly before Aleynikov left Goldman, there was an outage that made access to source code unavailable at least for several hours that impacted developers' productivity. This information will aid the defense in demonstrating that Aleynikov did not have the specific intent necessary to commit the crimes with which he was been charged. These Items relate to a short, discrete time period, and the Items are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

22. The content of the /local/tws/rv* directory as of 6/5/2009 on tws-stock-c1 and tws-stock-c5 hosts.

The Indictment alleges that Aleynikov downloaded materials other than what he was assigned to work on. The directories requested in Item 22 contain log files Aleynikov generated to understand traffic patterns between components of the trading platform. These log files will demonstrate that one of the tasks Aleynikov was assigned was to improve efficiency of the trading platform by decreasing the overall load on the network. The defense will use these logs at trial to demonstrate that given his responsibility to reduce network traffic, Aleynikov had to assess the contribution to network load presented by many of the Platform's components represented by source code files he was not otherwise responsible for coding. This request is very specific, relating to a single day, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

23. The CVS log history of every file in the eq/twscore and eq/tsecdb packages in the interval of 1/1/2008 to 6/5/2009.

Items 23 is relevant to demonstrate that Aleynikov did not intend to convert Goldman's alleged trade secret to his or anyone else's economic benefit — an element the government must prove beyond a reasonable doubt to establish a violation of the EEA. 18 U.S.C. § 1832(a)(2). Each of the components of the Platform has a modification history. This log file will show that the volatility for certain components is high (i.e., the components are modified frequently). By showing the relative instability of the elements Aleynikov transferred, the defense will show that the items he transferred in June 2009 would have had little or no value by July 2009 because they were already outdated. This request is very specific — relating to only two packages on the

Platform — and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

24. Slang source code extract of all scripts that have "TSecDb", "Nasdaq" or "TsAlgo" as part of the name (as of 6/5/2009) and/or reference scripts that contain "Nasdaq" keyword.

A large portion of Goldman's trading platform is written in a special programming language developed at Goldman known as "Slang". The defense will show that to the extent the Platform contains any trade secrets, they were in the trading engine and algorithms, which were written in Slang. The materials requested in Item 24 will enable the defense to establish the function of this code. It will also enable the defense to establish that Aleynikov had access to all such code, but did not attempt to obtain it. This proof will enable the defense to rebut the Government's claim of specific intent by showing that Aleynikov did not download arguably the most valuable aspect of the Platform. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

25. The full content of all files and subdirectories of the /hull3/prod/data directory as of 6/5/2009.

The production configuration information requested through this demand will identify the files that are required to get the Platform up and running. The Platform's source code could not be used by a third party without the configuration details stored in the above-mentioned locations. This will enable the defense to show that Aleynikov did not transfer any of these files in his download. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion

to dismiss the Indictment for insufficient evidence.

26. A full recursive list of all files found in the directory and all subdirectories of /hull3/prod/bin (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

The Platform consists of a number of executable files that run in the production environment in order to monitor market events and make trading decisions. This list of all executable files that represent the Platform and their dependencies will show that Aleynikov never took the executable files or their dependencies. The defense will show that one would have to take these files if he intended to run the Platform outside of Goldman's environment. The material requested in Item 26 is relevant to Aleynikov's defense that he did not intend to convert any Goldman files to his economic benefit. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

27. Dump of all content of STOCK trading parameter tables from the Animal database (or the database that was used in production on 6/5/2009) in the STOCK production network on 6/5/2009.

The defense will show that these parameter tables are necessary to make fine-grain adjustments to the Platform's behavior, and that the other elements of the Platform would be unable to operate without them. The defense will further demonstrate that none of these tables was included in Aleynikov's file transfers and that this information would be impossible to reverse engineer. Given that the Platform cannot operate without these parameter tables, the absence of the tables in Aleynikov's transfer further supports the defense theory that he did not intend to convert any Goldman files to his economic benefit. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also

relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

28. Daily copies of the directory /tmp/aleyns of tws-spice-c12 and qtdev3 hosts between 3/1/2009 and 6/5/2009.

The defense will demonstrate at trial that Aleynikov regularly emailed or transferred files offsite as he diligently worked on software development from home, and to a local directory at Goldman so that he would be able to continue working in case of a network outage at Goldman. The records requested in Item 28 are the local copies of the transferred files. A review of the information requested through this demand will show that Aleynikov created a local copy of the files for use during his employment in case of a network outage. This evidence will thus enable Aleynikov to offer an innocent explanation for his behavior. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

29. Information security access lists of firewall or router ACLs enumerating outbound access restrictions of hosts in the STOCK development network in the form (from network address mask, protocol, outbound network and outbound port).

30. Information security access lists of firewall or router ACLs enumerating outbound access restrictions of STOCK hosts (i.e., tws-nsdq-stk-c1,2,3) in the Nasdaq co-located network.

In order to demonstrate that the code Aleynikov downloaded constituted a trade secret, as the Government must to establish that he violated the EEA, it must prove beyond a reasonable doubt that Goldman took reasonable measures to keep the information secret. United States v. Shiah, No. SA CR 06-92, 2008 U.S. Dist. LEXIS 11973 (C.D. Cal. Feb. 19, 2008). To challenge the reasonableness of Goldman's security measures, in turn, the defense must have documents from Goldman sufficient to evidence the measures the company actually took to keep the

Platform secret. Items 29 and 30 will enable the defense to compare the security restrictions implemented by Goldman in NASDAQ's co-located network with those implemented by Goldman in its mothership network to demonstrate that Goldman's measures permitted the types of uploads Aleynikov made in the mothership network, whereas in NASDAQ's network it would not have. To this extent, it will be possible to show that Goldman's information security personnel were capable of configuring networks to restrict outside access, yet did not take such protective measures in the mothership network to secure its alleged trade secrets. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

31. The UNIX group membership policies showing the group names of which the aleyns account was a part as of 6/5/2009.

The information requested in Item 31 will show the security groups to which Aleynikov had membership. This information will demonstrate that Aleynikov did not exceed his access as alleged in the Indictment and only accessed information he was entitled to access in the course of his employment. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

32. Records sufficient to indicate whether the aleyns account had root-level access rights in the STOCK development and production networks.

The defense will use these records to demonstrate that Aleynikov had root-level access to Goldman's production and development networks. This information will enable the defense to demonstrate that Aleynikov did not exceed his authorized access, as alleged in Count 3 of the

Indictment. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

33. Records sufficient to indicate whether the aleyns account or any other account Aleynikov was permitted to use had local administrative rights on Aleynikov's desktop at Goldman.

The defense will use these records to demonstrate that Aleynikov had root-level access on his desktop computer at Goldman. This information will enable the defense to demonstrate that Aleynikov did not exceed his access as alleged in Count 3 of the Indictment. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

34. A list of all firewall policies blocking any outbound http and https access either from Aleynikov's desktop or from any production/development networks.

In order to demonstrate that the code Aleynikov downloaded constituted a trade secret, as the Government must to establish that he violated the EEA, it must prove beyond a reasonable doubt that Goldman took reasonable measures to keep the information secret. Shiah, No. SA CR 06-92, 2008 U.S. Dist. LEXIS 11973 (C.D. Cal. Feb. 19, 2008). To challenge the reasonableness of Goldman's security measures, in turn, the defense must have documents from Goldman sufficient to evidence the measures the company actually took to keep the Platform secret. The defense will use these policies to show the extent to which Goldman did, or did not, implement security measures to secure its alleged trade secrets. This request is very specific, and the Items requested are not obtainable from any source other than Goldman. This request is also relevant

to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

35. Any and all patents Goldman possesses or owns covering or relating to any source code used in or comprising a component of the Platform.

The absence of any patent on the Platform will enable the defense to establish that it did not constitute a trade secret. Likewise, the existence of a patent on the Platform or any portion of it will show the extent to which Goldman believed it had a protectable intellectual property. Comparison of the files transferred by Aleynikov to the patented portions of the Platform, if any, will enable the defense to demonstrate that Aleynikov did not transfer any patented materials. This request is very specific. Although patents are publicly available, Goldman has superior knowledge regarding the existence of any patents on the Platform, and could easily identify relevant patent numbers or indicate that no relevant patents on the Platform exist. This request is also relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

36. A copy of the United States Department of Justice Checklist for Reporting a Theft of Trade Secrets Offense that was filed by Goldman regarding Aleynikov.

The document requested in Item 36 will contain Goldman's description of what it considers to be its trade secret, and the steps it took to protect it. Although the document, if it exists, would constitute Jencks Act material, Goldman should be compelled to produce it in response to the subpoena because it is relevant to Aleynikov's forthcoming motion to dismiss the Indictment for insufficient evidence.

CONCLUSION

For the reasons set forth above, defendant Sergey Aleynikov respectfully requests that the Court grant him approval, *nunc pro tunc*, to subpoena the documents and materials described in Exhibit A from Goldman Sachs & Company ("Goldman") for production directly to him by Goldman.

Dated: June 21, 2010
Chatham, New Jersey

Respectfully submitted,

MARINO, TORTORELLA & BOYLE, P.C.

By: /s/ Kevin H. Marino
Kevin H. Marino
437 Southern Boulevard
Chatham, New Jersey 07928-1488
(973) 824-9300
Attorneys for Defendant
Sergey Aleynikov

EXHIBIT A

EXHIBIT A

(Documents, Electronically Stored Information And Materials To Be Produced By Goldman Sachs & Company)

1. All computer files, programs, source code and other components comprising the high-frequency trading system (the "Platform") of Goldman Sachs & Co. ("Goldman").

2. Documents sufficient to evidence any and all measures taken by Goldman to maintain the secrecy, confidentiality and/or proprietary nature of the programs, files, source code and other components comprising the Platform.

3. All documents relating to any employee training provided by Goldman regarding the identification and protection of confidential and/or proprietary information and material.

4. All confidentiality and/or non-disclosure agreements that Sergey Aleynikov ("Aleynikov") executed or to which he was otherwise bound during his employment by Goldman.

5. All written confidentiality and/or non-disclosure policies of Goldman that were effective during Aleynikov's employment by Goldman, including but not limited to all policies mandating or evidencing any mandatory confidentiality legends required to accompany source code containing trade secrets.

6. All written policies of Goldman regarding the copying and/or use of computer source code, files and programs for working at home or otherwise outside of Goldman's premises that were effective during Aleynikov's employment by Goldman.

7. All written policies or procedures of Goldman relating to determining whether departing employees are in possession of any proprietary, confidential or trade secret information or material that were effective during Aleynikov's employment by Goldman.

8. All communications between Goldman and Teza Technologies LLC relating to Aleynikov and/or the Platform.

9. All communications between Goldman and the Federal Bureau of Investigations or the United States Attorney's Office for the Southern District of New York relating to Aleynikov and/or the Platform.

10. All documents relating to any investigation conducted by Goldman of Aleynikov and his alleged theft of the Platform.

11. The content of the https logs from the proxy server containing records from 3/1/2009 to 6/5/2009 showing originating and destination IPs (and host names) and the size of transferred data.

12. The IP addresses of all tws-spice-c1 through tws-spice-c12 machines and qtdev1 through qtdev6 machines as of 3/1/2009, 4/1/2009, 5/1/2009 and 6/5/2009.

13. The full content of all files and subdirectories of the /bld/dev directory as of 6/5/2009.

14. A full recursive list of all files found in the directory and all subdirectories of /bld/pre (showing file path, file name, file size, access permission mask, group name, and user name) as of 6/5/2009.

15. A full recursive list of all files found in the directory and all subdirectories of /bld/ver (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

16. A full recursive list of all files found in the directory and all subdirectories of /bld/prod (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

17. The full content of all files and subdirectories of the /sw/external/erlang-common directory as of 6/5/2009.

18. The full content of all files and subdirectories of the /sw/external/erlang directory as of 6/5/2009.

19. A full recursive list of all dependencies of the twscore and tsecdb packages as of 6/5/2009.

20. A full recursive list of all files found in the directory and all subdirectories of /sw/external (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

21. All MS Communicator chat records of the aleyns account between 5/20/2009 and 6/5/2009.

22. The content of the /local/tws/rv* directory as of 6/5/2009 on tws-stock-c1 and tws-stock-c5 hosts.

23. The CVS log history of every file in the eq/twscore and eq/tsecdb packages in the interval of 1/1/2008 to 6/5/2009.

24. Slang source code extract of all scripts that have “TSecDb”, “Nasdaq” or “TsAlgo” as part of the name (as of 6/5/2009) and/or reference scripts that contain “Nasdaq” keyword.

25. The full content of all files and subdirectories of the /hull3/prod/data directory as of 6/5/2009.

26. A full recursive list of all files found in the directory and all subdirectories of /hull3/prod/bin (showing file path, file name, file size, access permission mask, group name and user name) as of 6/5/2009.

27. Dump of all content of STOCK trading parameter tables from the Animal database (or the database that was used in production on 6/5/2009) in the STOCK production network on 6/5/2009.

28. Daily copies of the directory /tmp/aleyns of tws-spice-c12 and qtdev3 hosts between 3/1/2009 and 6/5/2009.

29. Information security access lists of firewall or router ACLs enumerating outbound access restrictions of hosts in the STOCK development network in the form (from network address mask, protocol, outbound network and outbound port).

30. Information security access lists of firewall or router ACLs enumerating outbound access restrictions of STOCK hosts (i.e., tws-nsdq-stk-c1,2,3) in the Nasdaq co-located network.

31. The UNIX group membership policies showing the group names of which the aleyns account was a part as of 6/5/2009.

32. Records sufficient to indicate whether the aleyns account had root-level access rights in the STOCK development and production networks.

33. Records sufficient to indicate whether the aleyns account or any other account Aleynikov was permitted to use had local administrative rights on Aleynikov's desktop at Goldman.

34. A list of all firewall policies blocking any outbound http and https access either from Aleynikov's desktop or from any production/development networks.

35. Any and all patents Goldman possesses or owns covering or relating to any source code used in or comprising a component of the Platform.

36. A copy of the United States Department of Justice Checklist for Reporting a Theft of Trade Secrets Offense that was filed by Goldman regarding Aleynikov.